(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 April 2005 (07.04.2005)

PCT

(10) International Publication Number
WO 2005/031544 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number:
PCT/US2004/031745

(22) International Filing Date:
27 September 2004 (27.09.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/481,428	26 September 2003 (26.09.2003)	US
10/___,___	27 September 2004 (27.09.2004)	US

(71) Applicant *(for all designated States except US)*: **DISNEY ENTERPRISES, INC.** [US/US]; 500 South Buena Vista Street, Room 111K, Burbank, California 91521-0158 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **ACKLEY, Jonathan Michael** [US/US]; 1729 Ben Lomond Drive, Glendale, California 90102 (US).

(74) Agents: **GREENBERG TRAURIG LLP** et al.; 2450 Colorado Avenue, Suite 400E, Santa Monica, California 90404 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: CELL PHONE PARENTAL CONTROL

(57) Abstract: A method for allowing remote control of the usage of a networked wireless device including incoming communications, outgoing communications, and application launching. Controlling entities, such as parent cellular telephones or web sites, are provided with the ability to select a list of approved anytime incoming communications, or approved incoming and outgoing communications based on time and day. Incoming communications include text messaging and telephone calls. Further, the controlling entity is provided with the ability to reroute to the controlling entity any usage of the wireless device such as incoming communications, outgoing communications, and application launching. Access to usage logs of the wireless device is provided to the controlling entity.

WO 2005/031544 A2

CELL PHONE PARENTAL CONTROL

BY

JONATHAN ACKLEY

BACKGROUND OF THE DISCLOSURE

[0001] Field of the Disclosure

[0002] The present disclosure relates to communication systems and methods with monitoring and control functions. In particular, it relates to communication systems with parental control and supervision of a child's wireless device usage.

[0003] State of the Art

[0004] There are several concerns preventing parents from purchasing cellular telephones for their children. One concern is that the child will abuse her calling privileges by calling accidentally or inappropriately resulting in high bills. Another important concern is that an stranger adult may attempt to contact the child though her cellular telephone without the knowledge and consent of the parent. The natural fear is the stranger may be kidnapper or abuser. A further concern is that the child will lose or misplace the handheld telephone device. An unauthorized user could potentially benefit from gratuitous telephone calls that the parent will have to ultimately pay.

[0005] Modern cellular telephones offer games and other entertainment applications. Parents may be hesitant to provide portable game platforms to children as the games might prove distracting during other activities.

[0006] Some cellular telephones are equipped with ground positioning system (GPS) microcontrollers providing information about the location of the cellular phone. GPS services might be used to help safeguard children, but currently the handsets are too expensive for mass-market consumption.

[0007] There are applications whereby a parent may specify a cap on the amount an account can spend per month. There are also systems that allow parents to

program telephone numbers and universal remote locator (URL) links as forbidden or restricted call destinations.

[0008] While these systems provide a useful manner for controlling cellular phones, they generally present limitations that have not been addressed until now. The first and most impacting limitation is the inability of the current systems to allow the parent to control the incoming phone calls. Parent may wish to limit incoming phone calls of adult strangers to protect their children from being victims of criminal activity, to limit the distractions she gets from friends such as invitations to play games on the internet, to alleviate a child from telemarketers interruptions, or to simply reduce the total usage time of the child.

[0009] A second limitation of current systems is that they do not allow for a time-based control of telephone applications and calls. While previous systems provided parents with the ability of restricting a number to call, for instance, they did not provide parents with the ability to restrict those numbers for particular periods of time. A third limitation of current systems is that they do not allow parents to access the call history of the child's telephone from the parents hand held device. A fourth limitation is that parents do not have the means to reroute phone calls to their telephones based on certain criteria of the incoming call number or based on the time the call is made. Finally, yet another limitation is that current systems do not allow for parent to schedule events on their children's phones such as setting reminding messages for the child.

SUMMARY OF THE DISCLOSURE

[0010] A system and method for controlling usage of a wireless device, such as a personal data assistant (PDA) or a cellular telephone is disclosed. Usage of the wireless device encompasses outgoing and incoming communication as well as application usage. Outgoing or incoming communications may include electronic email, telephone calls, text messaging, universal resource locator (URL) requests, etc. A controlling device is provided with software that allows it to control usage of the wireless device. The controlling device is, for instance, a telephone, PDA, or personal computer comprising an application which provides a way to control the

wireless device. In one embodiment, the application runs on a controlling entity's wireless device. Alternatively, the application may be a web-based application. The system and method may for example be used by a controlling entity such as a parent, to control or manage use of a child's cellular telephone.

[0011] In one embodiment, the software in the controlling entity allows the parent to schedule restrictions based on time by identifying periods when the child may make use of the wireless device. For example, calls may be restricted based on time of day, such as during school hours, or day of the week, such as weekdays or weekends. The identified time restrictions are then transmitted to a network database to which the controlled wireless device has access rights. The wireless device is also provided with software that allows it to access the time restrictions in the permission database. Once the information is accessed, the software determines if the current time is within the allowed permitted times. Alternatively, the time restrictions imposed by the controlling entity may also be transmitted directly to the wireless device and stored in permission database residing in the wireless device.

[0012] In another embodiment, incoming communication to a wireless device is controlled by a controlling entity. Incoming communication may be controlled based upon an approved list of incoming communication sources. Incoming communication sources include, for example, telephone numbers, SMS addresses, email address, or other addresses. A total restriction may be imposed for receiving incoming calls in the wireless device. The controlling device transmits the forbidden number or name corresponding to the source of the call to the permission database. The permission database may reside in the network or in the wireless device. The wireless device then checks if the data corresponding to the source of the call is qualified in the permission database as a forbidden number. If so, the wireless device rejects an incoming communication attempt from the forbidden source every time it is made.

[0013] Furthermore, the operator of the wireless device may request that a particular incoming communication source be approved by the controlling entity. The controlling entity will receive the request and transmit the permission or disallowance

to the permission database. The permission database may reside in the network or in the wireless device. The wireless device then checks the permission database and determines whether it has permission to take the incoming call.

[0014] The usage of a wireless device may also be rerouted to the controlling device. Usage of the wireless device encompasses outgoing and incoming communication as well as application usage. Once a certain use has been restricted, the software in the wireless device reroutes the use to the controlling device. For instance, if it receives an incoming phone call, the incoming phone call will be rerouted to the controlling device if it is time-restricted or forbidden. If the wireless device receives an attempt to launch an application, and the application usage is forbidden or restricted at the time of the attempt, the wireless device will forward the attempt to the controlling entity notifying that an attempt to launch the application was made.

[0015] In yet another embodiment, a controlling entity is capable of viewing usage information of a wireless device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0016] The disclosure will be better understood and objects, other than those set forth above, will become apparent when consideration is given to the following detailed description. Such description makes reference to the accompanying drawings wherein:

[0017] Figure 1 shows a component diagram of a parental control system in an illustrative embodiment incorporating features of the present disclosure.

[0018] Figure 2 shows a flow diagram of a parental control system for restricting incoming calls to a wireless device in an illustrative embodiment incorporating features of the present disclosure.

[0019] Figure 3 shows a flow diagram of a parental control system for receiving approved incoming calls to a wireless device in an illustrative embodiment incorporating features of the present disclosure.

[0020] Figure 4 shows a flow diagram of a parental control system for time restricting a particular use of a wireless device in an illustrative embodiment incorporating features of the present disclosure.

[0021] Figure 5 shows a flow diagram of a parental control system for attempting a particular use that has been time-restricted in wireless device in an illustrative embodiment incorporating features of the present disclosure.

DETAILED DESCRIPTION

[0022] In the following description, numerous specific details are set forth in order to provide a more thorough disclosure. It will be apparent, however, to one skilled in the art, that the art disclosed may be practiced without these specific details. In some instances, well-known features may have not been described in detail so as not to obscure the art disclosed.

[0023] There is at least a method and system to remotely control the usage of a wireless device. Usage of the wireless device includes incoming communication, outgoing communication, and wireless device application usage. A common situation that benefits from the remote control of a wireless device is where parents want to control their children's usage of wireless devices.

[0024] Communication between devices

[0025] The present disclosure is enabled by a system of communication between the controlling device (e.g. parent device) and the wireless device (e.g. child device). In one embodiment, as shown in Figure 1, a controlling device, namely a parent device 100, sends a controlling message to a child device 150. An SMS client 110 residing on the parent device generates a coded SMS message. The parent device sends the generated SMS message to a hosting SMSC (Short Message Service Center) 120. In turn, the SMSC routes the message to the message server 130. The message contains routing and destination information. The message server 130 is a program running on a separate computing device. The message server 130 verifies, via a database 140 that the sending entity is authorized to request data from the child device 150. The message server 130 then forwards the message via the SMSC 120 to the child device 150.

[0026] An SMS client in the child device 150 examines all incoming SMS messages. When a properly coded SMS message arrives, the SMS sniffer on the child device 130 decides which application the message is requesting. The appropriate application is launched in the child device and passes to that application the appropriate data encoded within the incoming SMS string from the parent device 100.

[0027] The client application then examines the request embedded in the SMS string and decides how it should react to the incoming request. This program is configured to access and edit files contained within the handset, including memory cards and other peripherals. Based on the request, the program can modify files, set device attributes or settings. It can also read information stored in the device, collate it and send it back to the parent device 100. If desired, these programs can make themselves visible to the owner of the child device 150 by way of alerts or requests for input.

[0028] Control of incoming communication

[0029] According to one embodiment, the parent device controls the settings for incoming communication to the child device. Incoming communications may constitute phone calls, short message service (SMS) text messages, etc.

[0030] In one embodiment, as shown in Figure 2, a parent may choose to limit incoming calls to their child by making sure the child may only receive calls at anytime from approved numbers. As way of example, a mother may control what incoming text messages her daughter Amy receives. She may add Sue's telephone number--Amy's best friend--to a list of allowed incoming communications. To do so, the mother selects an icon representing her daughter's device 210 and further selects the option "Add New Phone Number" 220. She then inputs Sue's name 230 and number 240. In addition, she checks options to allow text messages 250 as well as phone calls to be received by Amy's device 260. Subsequently she confirms the settings. An SMS message is sent to Amy's device which adds Sue's telephone number to the list of authorized incoming phone numbers 270. Now Amy can receive text messages from Sue. The parent may also control whether the child

device displays a notification that a previously unauthorized incoming number is now authorized 280.

[0031] In Figure 3, the child device receives an incoming communication 310. On Amy's handset there is an embedded list or database of authorized incoming numbers. When a communication attempt is received on the child device, an associated phone number is also received with the communication attempt 315. The handset receiver program checks the number received in the list of authorized incoming numbers 320. If the number is in the list (e.g. Sue's number), the communication is received 350. Otherwise the communication is rejected 330. The parent may also control whether the child device displays a notification that an unauthorized incoming communication attempt has been rejected 340.

[0032] In another embodiment, as shown in Figure 4, a parent may approve or restrict incoming communication during specified periods of time. For instance, Amy's mother may approve incoming text messaging from Sue only during non-school hours, and further, she may approve incoming phone calls only during the weekends. To do so, the mother selects an icon representing her daughter's device 410 and further selects the option "Set authorized incoming communication times" 420. She then selects from a list of preauthorized phone numbers selecting he daughters' friend Sue 430. The mother the selects the days in the week incoming calls from Sue are permitted 440. Further, she enters the times in the day at which calls may be allowed 450. In addition, she enters a schedule for authorized incoming text messages 460. Subsequently she confirms the settings. An SMS message is sent to Amy's device which sets the incoming call authorized schedule for Sue's telephone number 470. The parent may also control whether the child device displays a notification that a previously authorized incoming number is now time-restricted 480.

[0033] Yet, in another embodiment, a parent may approve incoming communication upon the request of the child. In the situation where a child has a telephone number she wants to add to her device as an authorized incoming number, a message is sent to the parent who may then approve or disallow the phone number. The message may be in the form of an SMS message between

telephones, be sent to a designated email address, or be displayed on a central administrative web site used by the parents. The parent can then approve or decline to approve the phone number via the parent device. This response is sent back to the child device. The new number is added to the list of authorized calling if it was approved by the parent. For instance Amy's mother may approve incoming telephone calls from Sue after Amy requests permission to receive Sue's device calls.

[0034] In another embodiment, a parent may specifically forbid a particular number to ever be received as an incoming communication to the child device. The parent can give the device to a child with the peace of mind that comes from knowing that the child will not be put at risk by allowing the child to communicate with strangers.

[0035] In yet another embodiment, a parent may reroute any incoming unauthorized communication with the child device. The communication attempt is rerouted to the parent device or a parent-supervised answering service. Unauthorized communications include specifically forbidden numbers, communications from time-restricted numbers calling outside the window of authorization, unknown numbers, etc.

[0036] As Figure 5 demonstrates, when a communication attempt is received on the child device 510, an associated phone number is also received with the communication attempt 520. The handset receiver program checks the number received in the list of authorized incoming numbers. If the number is not in the list 530, or is not an authorized time for receiving the call 540, or is specifically forbidden 550, the communication and a message 560, 570, or 580 is then forwarded to the parent device, provided that the rerouting option is set on the child device. The parent may also control whether the child device displays a notification that an unauthorized incoming communication attempt has been rerouted 595.

[0037] In another embodiment, a parent may access a history log of authorized and unauthorized incoming communications. The parent would be able to see incoming phone numbers that were answered, rejected, or rerouted and the corresponding times.

[0038] Control of outgoing communication

[0039] According to one embodiment, the parent device controls the settings for outgoing communication from the child device. Outgoing communications may constitute phone calls, short message service (SMS) text messages, URL requests, etc.

[0040] A parent may approve or restrict outgoing communication during specified periods of time. For instance, Amy's mother may approve outgoing text messaging from Amy's friend, Sue, only during non-school hours, and further, she may approve outgoing phone calls only during the weekends. As Figure 4 shows, the mother selects an icon representing her daughter's device 410 and further selects the option "Set authorized outgoing communication times" 420. She then selects from a list of preauthorized phone numbers selecting he daughters' friend Sue 430. The mother then selects the days in the week outgoing calls to Sue are permitted 440. Further, she enters the times in the day at which calls may be made 450. In addition, she may enter a schedule for authorized outgoing text messages 460. Subsequently she confirms the settings. An SMS message is sent to Amy's device which sets the outgoing call authorized schedule for Sue's telephone number 470. The parent may also control whether the child device displays a notification that a previously authorized outgoing number is now time-restricted 480. Finally, the parent may also control whether the time restriction applies to one phone number in the list or to multiple numbers in the list.

[0041] On the child device resides a database containing a list of authorized outgoing numbers. The parent device or web site can add or delete numbers from this list via a messaging system such as SMS. When a phone number is selected on the child device and the child attempts to initiate the call, the handset dialing program checks the current number entered against the list of valid numbers. If it finds the number, the dialing program then checks the time and date at which the dialed number can be called or sent a message. If the current time and date falls within the permitted time and date the child device completes the call. If it does not fall within the permission window, the child device displays an alert indicating that it is not a valid time to call. The parent may also control whether the child device sends a notification to the parent device that an unauthorized outgoing communication attempt has been rejected.

[0042] In yet another embodiment, a parent may reroute any outgoing unauthorized communication from the child device. The communication attempt is rerouted to the parent device or a parent-supervised answering service. Unauthorized communications may include specifically forbidden numbers, communications occurring outside the window of authorization, unknown numbers, etc. When a communication attempt originates on the child device, the dialing program checks the number dialed in the list of authorized outgoing numbers. If the number is not in the list, or is not an authorized time for making the call, the communication is then forwarded to the parent device, provided that the rerouting option is set on the child device. The parent may also control whether the child device displays a notification that the unauthorized outgoing communication attempt has been rerouted.

[0043] In another embodiment, a parent may access a history log of authorized and unauthorized outgoing communications from the child device. The parent would be able to see outgoing numbers that were connected, rejected, or rerouted and the corresponding times.

[0044] In yet another embodiment of controlling outgoing communication, a parent may schedule a communication from the child device to the parent device. For example the parent may schedule a communication from the child device everyday after school is over. The communication could be an SMS message or a phone call. The parent can also sign up to receive wireless alerts on his device when his child has spent a set amount of money making phone calls or messaging.

[0045] Control of applications usage

[0046] According to one embodiment, the parent device controls the settings for usage of applications on the child device such as games.

[0047] In another embodiment, a parent may approve or restrict the usage of applications during specified periods of time. The approved times and dates are then associated with these applications. The parent manages the application usage through a communication system such as SMS. The parent can request a list of the current applications available on the child device. Then, from a web or handset interface they may associate the appropriate day, time and recurrence data. This

data is then sent to the child handset and stored in the embedded application list which is contained in a database.

[0048] As illustrated in Figure 6, the application or operating system that receives the request to launch the application first examines the data associated with that application 610. The application launcher retrieves the permitted times associated with the requested application 620 and compares the current time and date 630. The current time is provided through the handset's operating system or time and date data retrieved via Internet or WAP protocols. If the launcher determines that the application is outside of the permitted usage window the program will not run. Instead, the holder of the child device will be informed that the application (e.g. game) is locked-out for the time being 650. Otherwise the application will be launched 640. For instance, Amy's mother may approve using the web browser during the weekend and disallow its usage during the weekdays.

[0049] In another embodiment, the application list and associated lockout times are stored on a server. When the child handset attempts to run an application, the launcher program in the device first loads the application management data via Internet Protocol, WAP or other communication interfaces. It then checks the current time and date against this data to determine whether the parent device has locked out this application.

[0050] In yet another embodiment, a parent may reroute any unauthorized attempt to launch an application on the child device. If the rerouting option is set on the child device, the launching attempt is rerouted to the parent device as a form of communication message telling the parent that the child device is attempting to launch a given application.

[0051] In another embodiment, a parent may access a history log of authorized and unauthorized launching of applications on the child device. The parent would be able to see outgoing numbers that were connected, rejected, or rerouted and the corresponding times.

[0052] In yet another embodiment of controlling application launching, a parent may schedule the launching of an application for a specific purpose. From a web or phone interface, the parent can schedule automated SMS reminders or reminder

phone calls. For instance, if the child has a piano lesson Wednesday after school, he gets a reminder weekly at 2:30 PM every Wednesday.

[0053] Although certain illustrative embodiments and methods have been disclosed herein, it will be apparent form the foregoing disclosure to those skilled in the art that variations and modifications of such embodiments and methods may be made without departing from the true spirit and scope of the art disclosed. Many other examples of the art disclosed exist, each differing from others in matters of detail only. For instance,

[0054] Similarly, it will be apparent to one skilled in the art, that the wireless devices may be a cell phone or any other SMS enabled device. Thus the nature of the wireless network on which it runs is irrelevant as long as it enables communication among the wireless devices. Other communication protocols may be used such as Code Division Multiple Access wireless networks (CDMA) or Global System for Mobile networks (GSM, GSM/GPRS), Enhanced Data-Rates for GSM Evolution (EDGE) network, Universal Mobile Telecommunications Service (UMTS) network, Wideband Code Division Multiple Access (W-CDMA) network, Time Division Multiple Access (TDMA) network, iDen or any network offering SMS or data connections such as TCP/IP.

[0055] Likewise, custom SMS client(s) resident in the device may be implemented in any standard computing language such as C, C++, Java, Java 2 Micro Edition, Brew, SIM Toolkit or written for Symbian or other software platform.

[0056] Furthermore, rather than SMS transport, communication can be through TCP/IP, WAP (Wireless Application Protocol), WAP Push, HTTP or other e-mail, Internet or mobile communication protocols. Also, for applications that do not require a high level of security, the message transport could be sent directly between two handsets, rather than going through the intermediary message server.

[0057] Finally, it will also be apparent to one skilled in the art that control of the child device by a parent device may be applicable to other situations where usage control is necessary such as employer device controlling an employee device.

[0058] Accordingly, it is intended that the art disclosed shall be limited only to the extent required by the appended claims and the rules and principles of applicable law.

WE CLAIM:

1. A time-based method of remotely controlling a particular use of a wireless device, the method comprising:

providing a first software to a controlling entity wherein the first software allows to schedule a usage time restriction by identifying periods of time when a particular usage of the controlled wireless device is allowed;

communicating the usage time restriction from the controlling entity to a networked permission database via the communications network;

storing the usage time restriction at the networked permission database; and

providing a second software to the wireless device wherein the second software is configured to:

retrieve the usage time restriction from the networked permission database to assess if the particular use of the wireless device is permitted; and

allow the particular use only during the usage time restriction.

2. The method of claim 1 wherein the period of time is a starting time in the day, and ending time in the day, and a day.

3. The method of claim 1 wherein the particular use of the wireless device is receiving an incoming communication

4. The method of claim 3 wherein the incoming communication is a text message

5. The method of claim 3 wherein the incoming communication is a telephone call.

6. The method of claim 3 wherein the incoming communication is an electronic mail.

7. The method of claim 1 wherein the particular use of the wireless device is sending an outgoing communication.

8. The method of claim 7 wherein the outgoing communication is a text message.

9. The method of claim 7 wherein the outgoing communication is a telephone call.

10. The method of claim 7 wherein the outgoing communication is a universal resource locator request.

11. The method of claim 7 wherein the outgoing communication is an electronic mail message.

12. The method of claim 1 wherein the particular use of the wireless device is launching applications in the wireless device.

13. The method of claim 1 wherein the wireless device is a cellular telephone.

14. The method of claim 1 wherein the wireless device is a personal digital assistant (PDA).

15. The method of claim 1 wherein the controlling entity is a cellular telephone.

16. The method of claim 1 wherein the controlling entity is a web based application.

17. The method of claim 1 wherein the controlling entity is a computer application.

18. The method of claim 1 wherein the first software is further configured to provide access to the controlled wireless device past usage information.

19. The method of claim 1 wherein the second software is further configured to display an alert indicating that the particular use is only allowed during the usage time restrictions.

20. The method of claim 1 wherein the networked permission database resides in the wireless device.

21. The method of claim 1 wherein the networked permission database resides in a database server.

22. A permission-based method of remotely controlling the use of a wireless device, the method comprising:

transmitting via a communications network a request from the wireless device to a controlling entity to permit an incoming communication from an incoming communication source;

providing a first software to a controlling entity wherein the first software is configured to:

formulating a response to the request; and

transmitting the response to a networked permission database via the communications network; and

providing a second software to the wireless device wherein the second software is configured to:

retrieve a permission from the networked permission database to communicate with the incoming communication source; and

communicate with the incoming communication source only after receiving the permission.

23. The method of claim 22 wherein the wireless device is a cellular telephone.

24. The method of claim 22 wherein the wireless device is a personal data assistant.

25. The method of claim 22 wherein the controlling entity is a cellular telephone.

26. The method of claim 22 wherein the controlling entity is a web based application.

27. The method of claim 22 wherein the controlling entity is a computer application.

28. The method of claim 22 wherein the incoming communication is a text message.

29. The method of claim 22 wherein the incoming communication is a telephone call.

30. The method of claim 22 wherein the incoming communication is an electronic mail message.

31. The method of claim 22 wherein the first software is further configured to access to the wireless device past usage information.

32. The method of claim 22 wherein the second software is further configured to display an alert indicating that the particular only allowed during the usage time restrictions.

33. A method of remotely controlling communications to a wireless device, the method comprising:

providing a first software to a controlling entity wherein the first software allows to determine an identifier for a forbidden incoming communication source;

transmitting the identifier from the controlling entity to a networked permission database via a communications network;

storing the identifier at the networked permission database; and

providing a second software to the wireless device wherein the second software is configured to:

retrieve from the networked permission database the identifier corresponding to the forbidden incoming communication source; and

reject communication attempts from the forbidden incoming communication source based on the identifier retrieved.

34. The method of claim 33 wherein the networked permission database resides in the wireless device.

35. The method of claim 33 wherein the networked permission database resides on a database server.

36. The method of claim 33 wherein the wireless device is a cellular telephone.

37. The method of claim 33 wherein the wireless device is a personal data assistant.

38. The method of claim 33 wherein the controlling entity is a cellular telephone.

40. The method of claim 33 wherein the controlling entity is a web based application.

41. The method of claim 33 wherein the controlling entity is a computer application.

42. The method of claim 33 wherein the incoming communication is a text message.

43. The method of claim 33 wherein the incoming communication is a telephone call.

44. The method of claim 33 wherein the incoming communication is an electronic mail message.

45. A method of remotely controlling a particular use of a wireless device, the method comprising:

providing a first software to a controlling entity wherein the first software allows to place a usage restriction on the wireless device;

communicating the usage time restriction from the controlling entity to a networked permission database via the communications network;

storing the usage time restrictions at the networked permission database; and

providing a second software to the wireless device wherein the second software is configured to:

retrieve the usage restriction from the networked permission database to assess if the particular use of the wireless device is permitted; and

allow the particular use only in compliance with the usage restrictions; and

forward the usage request from the wireless device to the controlling entity.

46. The method of claim 45 wherein the first software is further configured to provide access to the wireless device past usage information.

47. The method of claim 45 wherein the second software is further configured to display an alert indicating the communication attempt from the forbidden incoming communication source.

48. The method of claim 45 wherein the networked permission database resides in the wireless device.

49. The method of claim 45 wherein the networked permission database resides in a database server.

50. The method of claim 45 wherein the particular use of the wireless device is receiving incoming communication.

51. The method of claim 50 wherein the incoming communication is a text message.

52. The method of claim 50 wherein the incoming communication is a telephone call.

53. The method of claim 50 wherein the incoming communication is an electronic mail.

54. The method of claim 45 wherein the particular use of the wireless device is sending outgoing communication.

55. The method of claim 54 wherein the outgoing communication is a text message.

56. The method of claim 54 wherein the outgoing communication is a telephone call.

57. The method of claim 55 wherein the outgoing communication is a universal resource locator request.

58. The method of claim 55 wherein the outgoing communication is an electronic mail message.

59. The method of claim 45 wherein the wireless device is a cellular telephone.

60. The method of claim 45 wherein the wireless device is a personal data assistant.

61. The method of claim 45 wherein the particular use of the wireless device is launching applications in the wireless device.

62. The method of claim 45 wherein the controlling entity is a cellular telephone.

63. The method of claim 45 wherein the controlling entity is a web based application.

64. The method of claim 45 wherein the controlling entity is a computer application.

65. The method of claim 45 wherein the first software is further configured to provide access to the wireless device past usage information.

66. The method of claim 45 wherein the second software is further configured to display an alert indicating that the particular use is only allowed during the usage time restrictions.

67. The method of claim 45 wherein the second software is further configured to display an alert indicating that the particular use has been forwarded to the controlling entity.

68. The method of claim 45 wherein the networked permission database resides in the wireless device.

69. The method of claim 45 wherein the networked permission database resides on a database server.

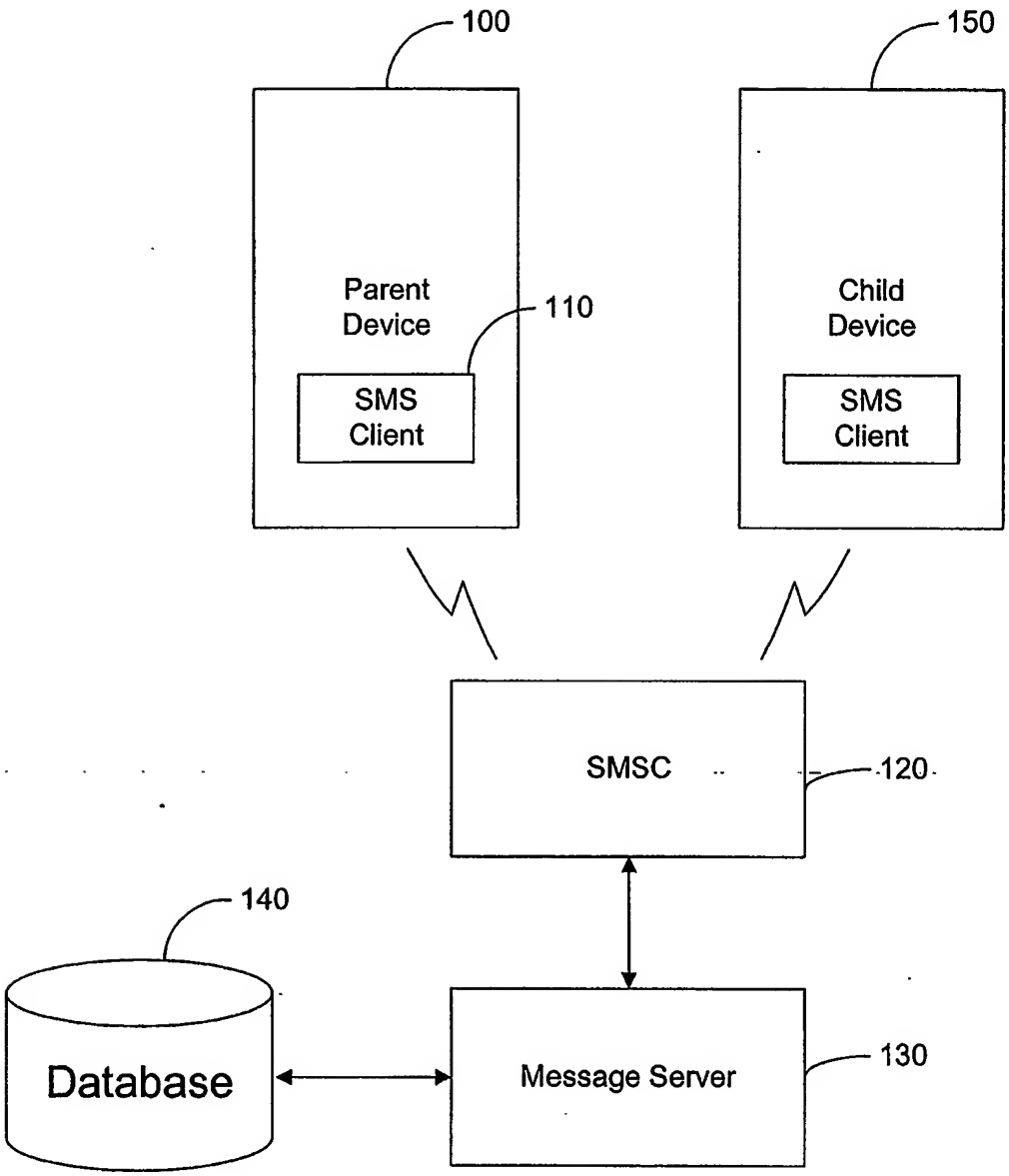
100
150
Parent Device
110
SMS Client
Child Device
SMS Client
SMSC
120
140
Database
Message Server
130

FIG. 1

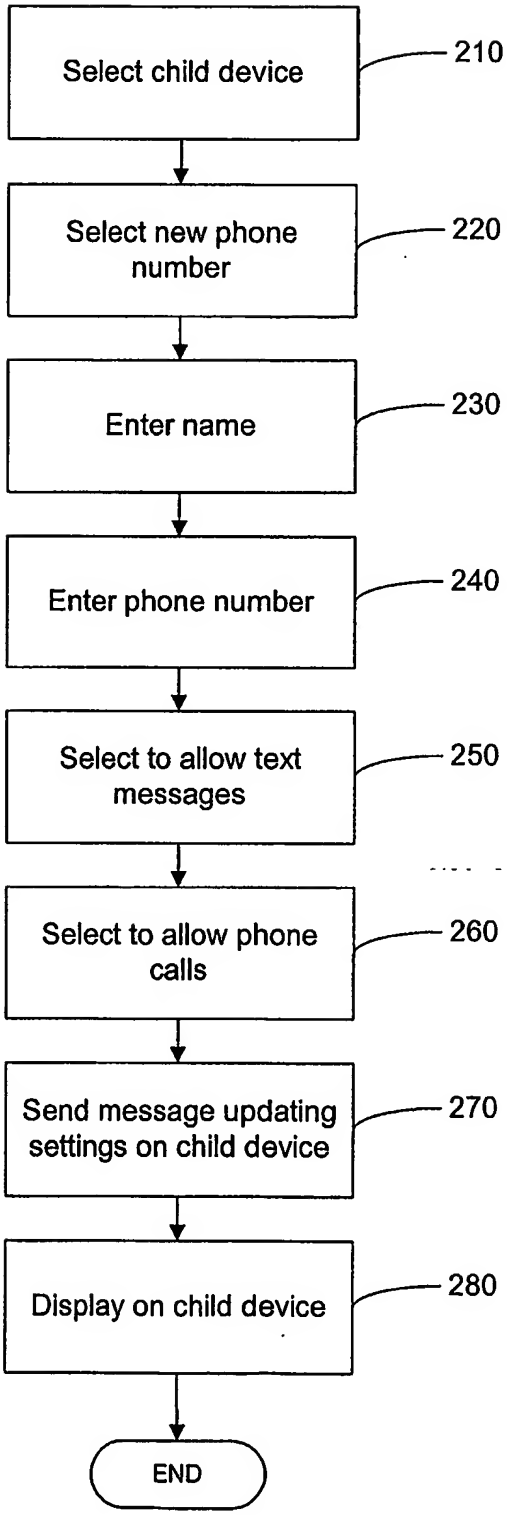

FIG. 2

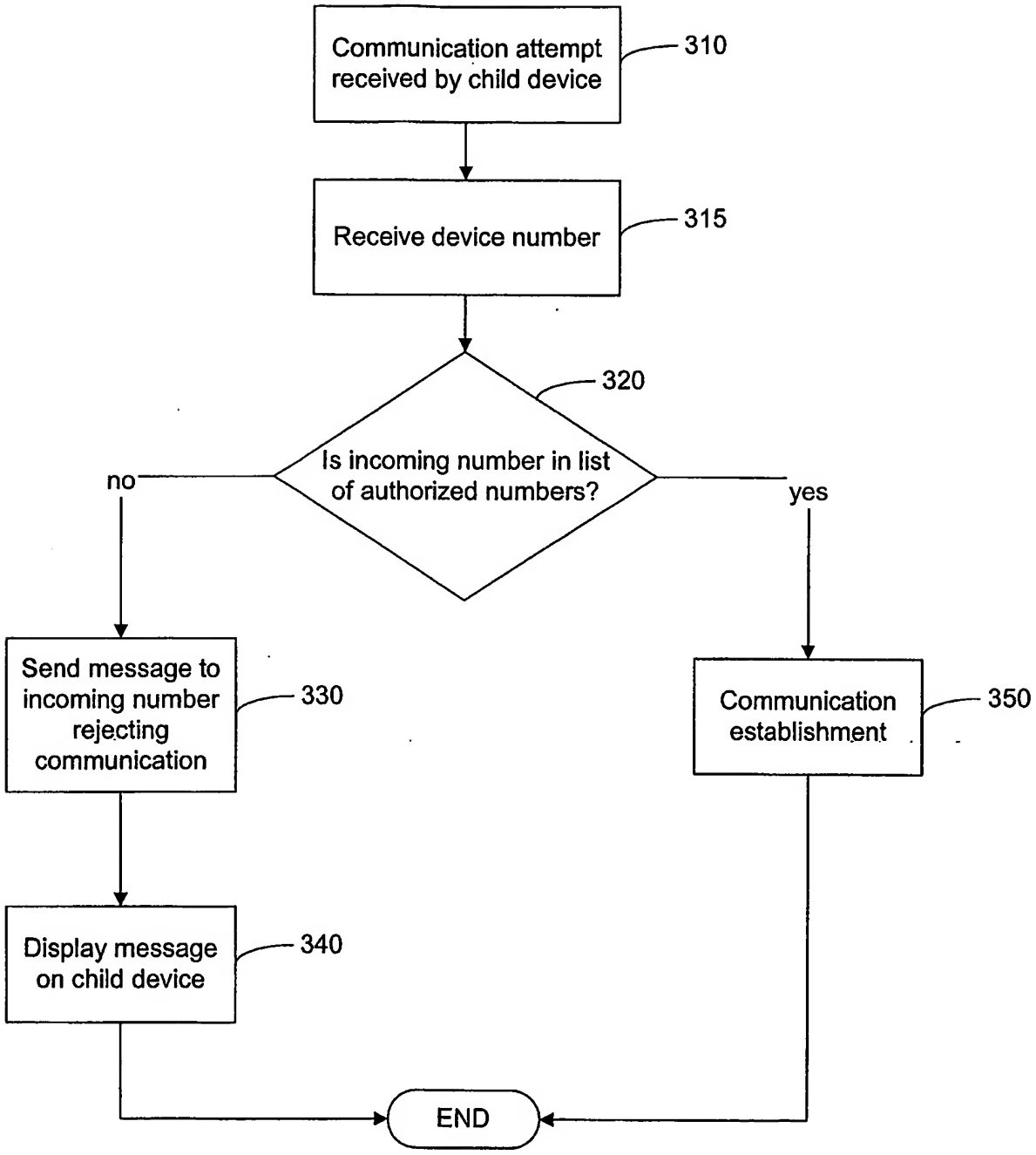
Communication attempt received by child device
310
Receive device number
315
320
Is incoming number in list of authorized numbers?
no
yes
Send message to incoming number rejecting communication
330
Communication establishment
350
Display message on child device
340
END

FIG. 3

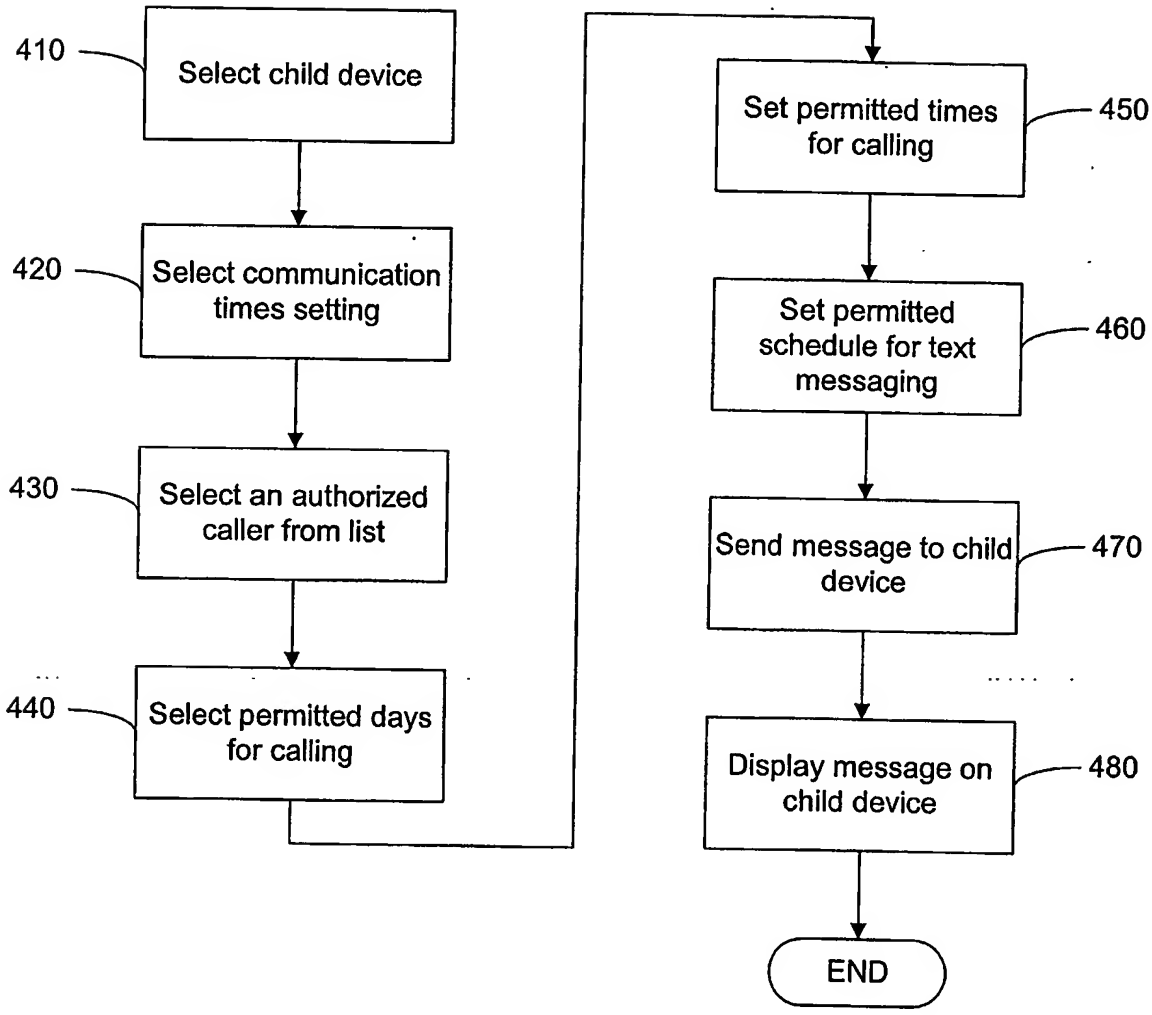
410
Select child device
420
Select communication times setting
430
Select an authorized caller from list
440
Select permitted days for calling
450
Set permitted times for calling
460
Set permitted schedule for text messaging
470
Send message to child device
480
Display message on child device
END

FIG. 4

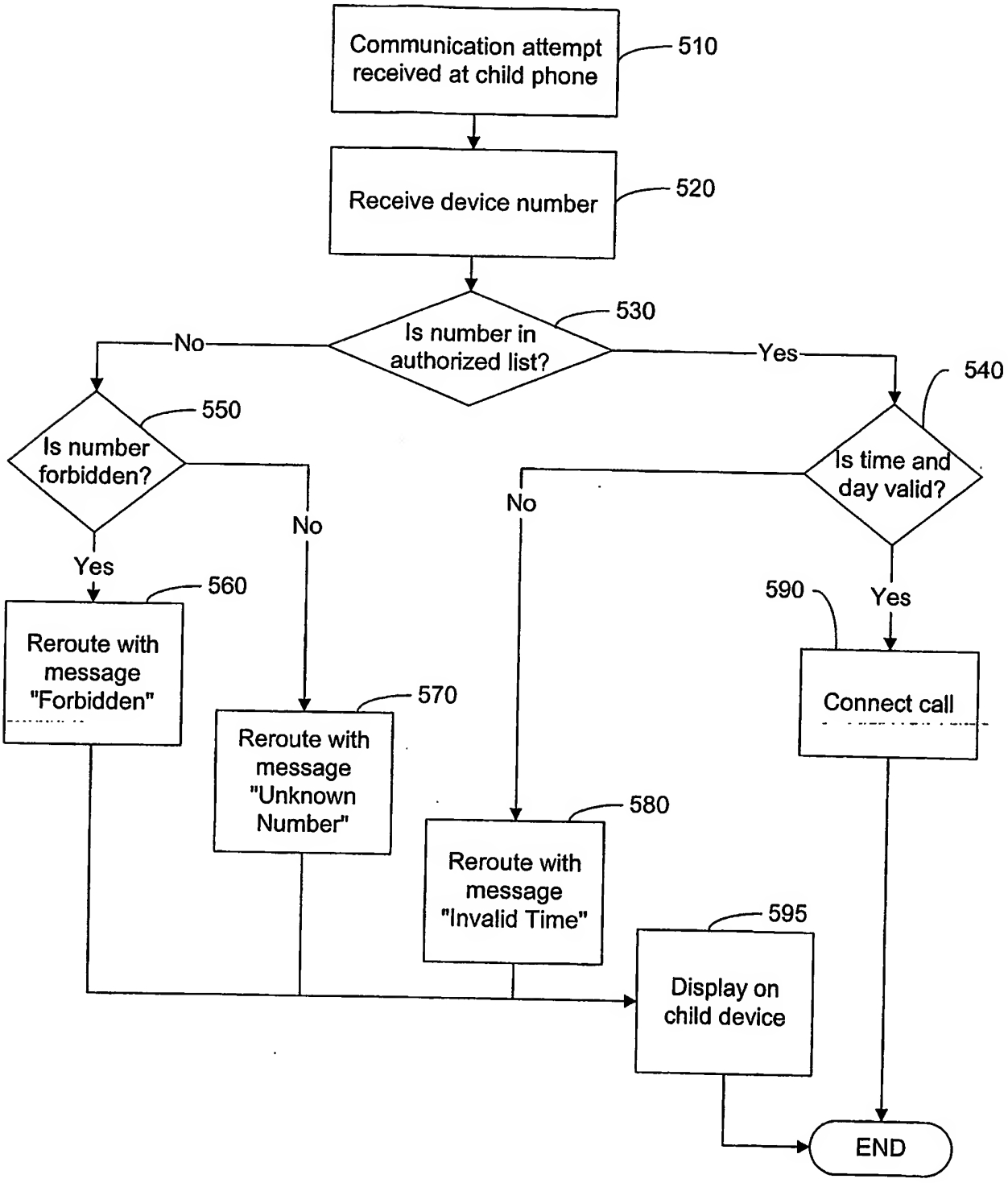
Communication attempt received at child phone
510
Receive device number
520
Is number in authorized list?
530
No
Yes
Is number forbidden?
550
Yes
No
Reroute with message "Forbidden"
560
Reroute with message "Unknown Number"
570
Is time and day valid?
540
No
Yes
590
Connect call
Reroute with message "Invalid Time"
580
Display on child device
595
END

FIG. 5

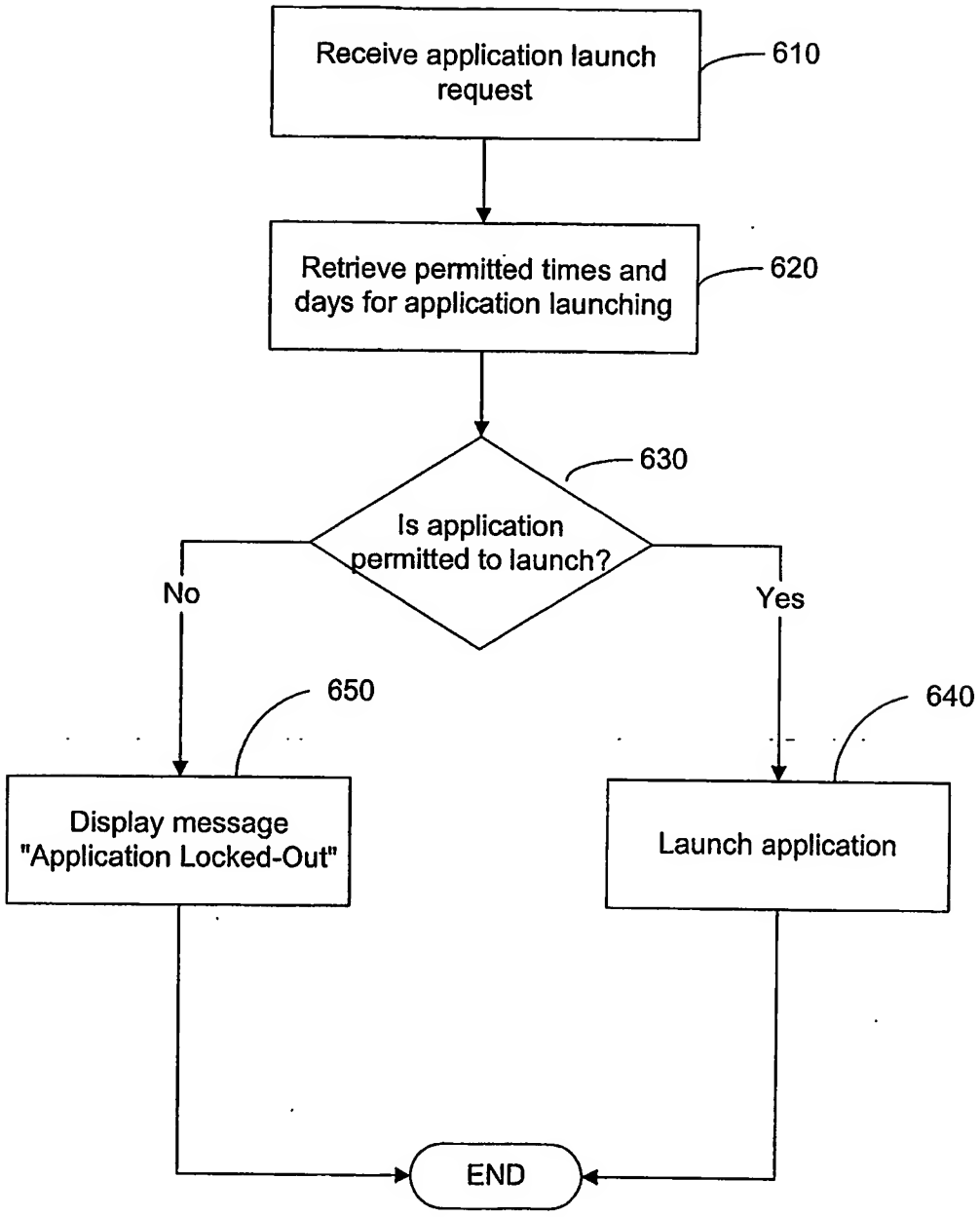

FIG. 6